

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-196546

(43)Date of publication of application : 14.07.2000

(51)Int.Cl.

H04H 1/00
H04B 1/16
H04N 7/16
H04N 7/167

(21)Application number : 10-371521

(71)Applicant : JISEDAI JOHO HOSO SYSTEM
KENKYUSHO:KK

(22)Date of filing : 25.12.1998

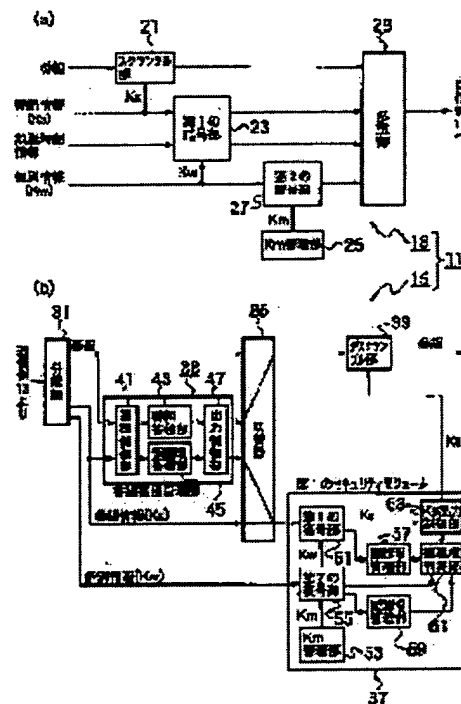
(72)Inventor : MACHIDA KAZUHIRO
KIMURA TAKESHI

(54) METHOD FOR TRANSMITTING/RECEIVING BROADCAST, BROADCAST TRANSMITTER, BROADCAST RECEIVER, AND BROADCAST TRANSMITTING/RECEIVING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make it possible to set an expiration date for each program without increasing individual information by adding the expiration date of a specific program to program information included in common information, broadcasting the period-added information, ciphering actual time information including actual broadcast time, and broadcasting the ciphered information.

SOLUTION: A 1st ciphering part 23 in a broadcast transmitter 13 adds viewing period information including the viewing period of a specific program to program information included in common information and ciphers actual time information including actual broadcast time. A viewing right judging part 61 in a broadcast receiver 15 executes period judgement related to whether the broadcast actual time acquired by decoding the actual time information extracted by a separation part 31 is included within the viewing period range of the specific program included in the viewing period information extracted by the separation part 31 or not. When viewing right exists, the original signal related to the specific program is restored by descrambling a scrambled signal extracted by the separation part 31.



LEGAL STATUS

[Date of request for examination]

06.04.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

【特許請求の範囲】

【請求項1】 映像、音声、又はデータ等を含む信号を放送する際に用いられる放送送受信方法であって、

放送送信側は、

少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、

放送受信側は、

前記スクランブル信号、前記視聴期限情報、及び前記実時間情報を受信したとき、当該受信した実時間情報を復号化することで取得した放送実時間が、前記受信した視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、

当該期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記受信したスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を実時間で視聴するストリーム型視聴を許可することを特徴とする放送送受信方法。

【請求項2】 映像、音声、又はデータ等を含む信号を放送する際に用いられる放送送受信方法であって、

放送送信側は、

少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、

放送受信側は、

前記スクランブル信号及び前記視聴期限情報を受信したとき、当該受信したスクランブル信号及び視聴期限情報を蓄積しておき、

当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、前記蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、当該期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴とする放送送受信方法。

【請求項3】 映像、音声、又はデータ等を含む信号を放送する際に用いられる放送送受信方法であって、

放送送信側は、

少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、

放送受信側は、

前記スクランブル信号及び前記視聴期限情報を受信したとき、当該受信したスクランブル信号及び視聴期限情報を蓄積しておき、

当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、前記蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う一方、前記放送実時間のうち、今回と前回の放送実時間の間で時間的な連続性が失われているか否かに係る連続性判定を行い、

前記期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下され、かつ、前記連続性判定の結果、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴とする放送送受信方法。

【請求項4】 映像、音声、又はデータ等を含む信号を放送する際に用いられる放送送受信方法であって、

放送送信側は、

少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、当該スクランブル信号の放送に先立って、個別情報に対して特定の基準値及び許容範囲を付加して放送する一方、前記スクランブル信号の放送に伴って、共通情報中の番組情報に対して前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加して放送し、

放送受信側は、

前記個別情報に付加された特定の基準値及び許容範囲を受信したとき、当該受信した特定の基準値を基礎として、前記受信した許容範囲から求められる第2の特定回数だけ前記放送送信側と共通の再帰的関数を用いて順次再帰的に生成した値を全てプールするとともに、前記スクランブル信号及び前記最終生成値を受信したとき、当該受信したスクランブル信号又は最終生成値を蓄積しておき、

当該蓄積されたスクランブル信号に係る特定の番組の再

生視聴要求を生じたとき、前記蓄積された最終生成値を基礎として前記再帰的関数を用いて再帰的に生成した1つの値と、前記プールしておいた全ての値とを順次比較することで、当該両者間で一致する値が存在するか否かに係る一致判定を行い、

このとき、前記特定の番組の再生視聴要求を生じる毎に、前記蓄積された最終生成値を、今回生成した1つの値に更新記憶し、

前記一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴とする放送受信方法。

【請求項5】 前記再帰的関数としては、一方向性のハッシュ関数が採用されることを特徴とする請求項4に記載の放送受信方法。

【請求項6】 映像、音声、又はデータ等を含む信号を放送する放送受信装置であって、

限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、

共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加する視聴期限情報付加手段と、

放送実時間を含む実時間情報を暗号化する実時間情報暗号化手段と、

前記スクランブル手段で生成したスクランブル信号と、前記視聴期限情報付加手段で視聴期限情報が付加された番組情報と、前記実時間情報暗号化手段で暗号化された実時間情報と、を多重化する多重化手段と、

を備え、前記多重化された放送信号を変調して放送することを特徴とする放送受信装置。

【請求項7】 映像、音声、又はデータ等を含む信号を放送する放送受信装置であって、

限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、

個別情報に対して特定の基準値及び許容範囲を付加する特定基準情報付加手段と、

共通情報中の番組情報に対し、前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加する最終生成値付加手段と、

前記スクランブル手段で生成したスクランブル信号と、前記特定基準情報付加手段で特定の基準値及び許容範囲が付加された個別情報と、前記最終生成値付加手段で最終生成値が付加された番組情報と、を多重化する多重化

手段と、

を備え、

前記多重化された放送信号を変調して放送する際に、前記個別情報は、前記スクランブル信号の放送に先立って放送される一方、前記最終生成値は、前記スクランブル信号の放送に伴って放送されることを特徴とする放送受信装置。

【請求項8】 前記再帰的関数としては、一方向性のハッシュ関数が採用されることを特徴とする請求項7に記載の放送受信装置。

【請求項9】 映像、音声、又はデータ等を含む放送信号を受信する放送受信装置であって、

限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、前記特定の番組の視聴期限を含む視聴期限情報、及び暗号化された放送実時間を含む実時間情報が多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、

当該分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記分離手段で取り出された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う期限判定手段と、

当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記分離手段で取り出されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、を備え、

前記デスクランブル手段は、

前記スクランブル信号に対するデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を実時間で視聴するストリーム型視聴を許可することを特徴とする放送受信装置。

【請求項10】 映像、音声、又はデータ等を含む放送信号を受信する放送受信装置であって、

限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、前記特定の番組の視聴期限を含む視聴期限情報、及び暗号化された放送実時間を含む実時間情報が多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、

当該分離手段で取り出されたスクランブル信号及び視聴期限情報を蓄積する番組蓄積手段と、

当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に前記分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記番組蓄積手段に蓄積された視聴期限情報に含まれる特定の番組の視聴

期限範囲内にあるか否かに係る期限判定を行う期限判定手段と、
当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、

を備え、

前記デスクランブル手段は、

前記スクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴とする放送受信装置。

【請求項11】 映像、音声、又はデータ等を含む放送信号を受信する放送受信装置であって、

限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、個別情報に付加された特定の基準値及び許容範囲、並びに共通情報中の番組情報に付加された前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値が多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、

当該分離手段で取り出された特定の基準値を基礎として、前記取り出された許容範囲から求められる第2の特定回数だけ前記再帰的関数を用いて順次再帰的に生成した値を全てプールする値プール手段と、

前記分離手段で取り出されたスクランブル信号又は最終生成値を蓄積する番組蓄積手段と、

当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、前記番組蓄積手段に蓄積された最終生成値を基礎として前記再帰的関数を用いて再帰的に生成した1つの値と、前記値プール手段にプールしておいた全ての値とを順次比較することで、当該両者間で一致する値が存在するか否かに係る一致判定を行う視聴権判定手段と、

前記特定の番組の再生視聴要求を生じる毎に、前記番組蓄積手段に蓄積された最終生成値を、前記視聴権判定手段で今回生成した1つの値に更新記憶する最終生成値更新記憶手段と、

当該視聴権判定手段における一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、

を備え、

前記デスクランブル手段は、

前記スクランブル信号に対してデスクランブル処理を施

すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴とする放送受信装置。

【請求項12】 前記再帰的関数としては、一方性のハッシュ関数が採用されることを特徴とする請求項11に記載の放送受信装置。

【請求項13】 映像、音声、又はデータ等を含む信号を放送する放送送信装置と、当該放送送信装置から放送された信号を受信する放送受信装置とを含んで構成される放送送信システムであって、

前記放送送信装置は、

限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、

共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加する視聴期限情報付加手段と、

放送実時間を含む実時間情報を暗号化する実時間情報暗号化手段と、

前記スクランブル手段で生成したスクランブル信号と、前記視聴期限情報付加手段で視聴期限情報が付加された番組情報と、前記実時間情報暗号化手段で暗号化された実時間情報と、を多重化する多重化手段と、

を備え、

前記多重化された放送信号を変調して放送し、

前記放送受信装置は、

前記多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、

当該分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記分離手段で取り出された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う期限判定手段と、

当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記分離手段で取り出されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、

を備え、

前記デスクランブル手段は、

前記スクランブル信号に対するデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を実時間で視聴するストリーム型視聴を許可することを特徴とする放送送信システム。

【請求項14】 映像、音声、又はデータ等を含む信号を放送する放送送信装置と、当該放送送信装置から放送された信号を受信する放送受信装置とを含んで構成される放送送信システムであって、

前記放送送信装置は、

限定受信対象となる特定の番組に係る原信号に対してス

クランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、

共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加する視聴期限情報付加手段と、

放送実時間を含む実時間情報を暗号化する実時間情報暗号化手段と、

前記スクランブル手段で生成したスクランブル信号と、前記視聴期限情報付加手段で視聴期限情報が付加された番組情報と、前記実時間情報暗号化手段で暗号化された実時間情報と、を多重化する多重化手段と、

を備え、

前記多重化された放送信号を変調して放送し、

前記放送受信装置は、

前記多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、

当該分離手段で取り出されたスクランブル信号及び視聴期限情報を蓄積する番組蓄積手段と、

当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に前記分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記番組蓄積手段に蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う期限判定手段と、

当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、

を備え、

前記デスクランブル手段は、

前記スクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴とする放送送受信システム。

【請求項15】 映像、音声、又はデータ等を含む信号を放送する放送送信装置と、当該放送送信装置から放送された信号を受信する放送受信装置とを含んで構成される放送送受信システムであって、

前記放送送信装置は、

限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、

個別情報に対して特定の基準値及び許容範囲を付加する特定基準情報付加手段と、

共通情報中の番組情報に対し、前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰

的に生成した値のうちの最終生成値を付加する最終生成値付加手段と、

前記スクランブル手段で生成したスクランブル信号と、前記特定基準情報付加手段で特定の基準値及び許容範囲が付加された個別情報と、前記最終生成値付加手段で最終生成値が付加された番組情報と、を多重化する多重化手段と、

を備え、

前記多重化された放送信号を変調して放送する際に、前記個別情報は、前記スクランブル信号の放送に先立って放送される一方、前記最終生成値は、前記スクランブル信号の放送に伴って放送され、

前記放送受信装置は、

前記多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、

当該分離手段で取り出された特定の基準値を基礎として、前記取り出された許容範囲から求められる第2の特定回数だけ前記放送送信装置と共通の再帰的関数を用いて順次再帰的に生成した値を全てプールする値プール手段と、

前記分離手段で取り出されたスクランブル信号又は最終生成値を蓄積する番組蓄積手段と、

当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、前記番組蓄積手段に蓄積された最終生成値を基礎として前記再帰的関数を用いて再帰的に生成した1つの値と、前記値プール手段にプールしておいた全ての値とを順次比較することで、当該両者間で一致する値が存在するか否かに係る一致判定を行う視聴権判定手段と、

前記特定の番組の再生視聴要求を生じる毎に、前記番組蓄積手段に蓄積された最終生成値を、前記視聴権判定手段で今回生成した1つの値に更新記憶する最終生成値更新記憶手段と、

当該視聴権判定手段における一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、

を備え、

前記デスクランブル手段は、

前記スクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴とする放送送受信システム。

【請求項16】 前記再帰的関数としては、一方向性のハッシュ関数が採用されることを特徴とする請求項15に記載の放送送受信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、限定受信対象となる特定の番組に係る信号を放送する際に用いられる放送受信方法に係り、特に、個別情報の量を増大させることなく、個々の番組毎に視聴期限を設定可能な放送受信方法、放送送信装置、放送受信装置、及び放送受信システムに関する。

【0002】また、本発明は、受信した番組を蓄積後に再生視聴する蓄積型視聴を行う場合であっても、放送事業者側の意図に反した視聴を可及的に抑制可能な放送受信方法、放送送信装置、放送受信装置、及び放送受信システムに関する。

【0003】

【従来の技術】最近時、既存の地上波放送に加えて、例えば、デジタル衛星放送やインターネット情報放送などを含む情報放送に係る社会基盤が急速に整備されつつある。

【0004】このような社会基盤を用いて、放送事業者は、映像、音声、又はデータ等を含む番組を視聴者宛に放送することを事業としているが、例えば民間の放送事業者が番組放送サービスを提供する対価として収入を得る際に、主として2つの仕組みが存在する。

【0005】一方は、提供スポンサーからCM料金の出資を受けて、提供スポンサーのCMを含む番組を、全ての視聴者に無料で提供する仕組みであり、他方は、視聴者毎の番組嗜好が多様化している実情に鑑みて、視聴者毎の多様な嗜好に応える番組を、視聴契約を結んだ契約視聴者に限定して有料で提供する仕組みである。

【0006】ここで、後者の仕組みを実現する手法として、例えば有料放送番組等の特定の番組を、契約視聴者のみに限定して受信させる限定受信方式が一般に知られている。

【0007】この限定受信方式の概要について述べると、放送送信側は、限定受信対象となる特定の番組を、その映像、音声、又はデータ等を含む原放送信号に対し、契約視聴者のみが取得し得るスクランブル鍵を用いてスクランブル処理を施したスクランブル信号を放送する一方、契約視聴者に属する放送受信側は、受信したスクランブル信号に対し、取得したデスクランブル鍵を用いたデスクランブル処理を施すことで特定の番組に係る原放送信号を復元する。

【0008】ここで、契約視聴者に属する放送受信側におけるデスクランブル処理の流れについて、受信した番組を実時間で視聴するストリーム型視聴と、受信した番組を蓄積後に再生視聴する蓄積型視聴とに分けて、さらに詳しく説明する。

【0009】まず、ストリーム型視聴では、放送受信側は、契約視聴者により特定の番組が選択されることで特定の番組の視聴要求が生じると、特定の番組に伴って放送されている、特定の番組に対応する共通情報ECM中の番組情報に含まれるティア情報（以下、契約情報と言

う。）及び放送実時間情報と、放送事業者から周期的に送信されることで前もって受信している個別情報ECM中の契約情報及び契約情報に含まれる視聴期限情報とを比較し、特定の番組が視聴契約対象であり、かつ放送実時間が視聴期限範囲内にあれば、放送送信側から受信した特定の番組に係るスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元する。

【0010】一方、蓄積型視聴では、放送受信側は、特定の番組の視聴制限を解除することなくスクランブル状態を維持したままで、受信した特定の番組を共通情報ECM中の番組情報とともに蓄積しておき、蓄積しておいた特定の番組を選択的に視聴する場合には、特定の番組とともに蓄積しておいた共通情報ECM中の番組情報に含まれる契約情報及び放送実時間情報と、前もって受信している個別情報ECM中の契約情報及び契約情報に含まれる視聴期限情報とを比較し、選択した特定の番組が蓄積時点で視聴契約対象であり、かつ蓄積時点における放送実時間が視聴期限範囲内にあれば、放送送信側から受信した特定の番組に係るスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元する。

【0011】

【発明が解決しようとする課題】しかしながら、上述した従来の契約視聴者側の放送受信装置で実行されるデスクランブル処理にあつては、下記に述べる複数の課題を内在していた。

【0012】すなわち、第1に、ストリーム型視聴と蓄積型視聴との両者に共通して、視聴期限は、個別情報ECM中の契約情報に対して設定されるため、個々の番組毎に視聴期限を設定することはできない。この課題を解決するために、番組毎に契約情報を持たせることも考えられるが、この場合、放送事業者から周期的に前もって送信しておかなければならない個別情報ECMの量が増大するといった新たな課題を生じてしまう。

【0013】第2に、蓄積型視聴を行う場合におけるスクランブルの解除条件として、選択した特定の番組が蓄積時点で視聴契約対象であり、かつ蓄積時点における放送実時間が視聴期限範囲内にあれば、スクランブルを解除することとしていたために、個別情報ECM中の契約情報及び契約情報に含まれる視聴期限情報が放送受信装置内に蓄積されており、かつ特定の番組を蓄積した時点でスクランブルの解除条件を満たしてさえいれば、特定の番組を何回でも視聴可能となる結果として、放送事業者側の意図に反した視聴を許すことになってしまう。

【0014】そこで、個別情報の量を増大させることなく、個々の番組毎に視聴期限を設定することができ、しかも、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した視聴を可及的に抑制可能な新規な技術の開発が関係者の間で久しく待ち望まれていた。

【0015】本発明は、上述した課題を解決するためになされたものであり、個別情報の量を増大させることなく、個々の番組毎に視聴期限を設定できる放送受信方法、放送送信装置、放送受信装置、及び放送受信システムを提供することを課題とする。

【0016】また、本発明は、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制し得る放送受信方法、放送送信装置、放送受信装置、及び放送受信システムを提供することを課題とする。

【0017】

【課題を解決するための手段】上記課題を解決するために、請求項1の発明は、映像、音声、又はデータ等を含む信号を放送する際に用いられる放送受信方法であって、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、放送受信側は、前記スクランブル信号、前記視聴期限情報、及び前記実時間情報を受信したとき、当該受信した実時間情報を復号化することで取得した放送実時間が、前記受信した視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、当該期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記受信したスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を実時間で視聴するストリーム型視聴を許可することを要旨とする。

【0018】請求項1の発明によれば、まず、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送する。

【0019】一方、放送受信側は、スクランブル信号、視聴期限情報、及び実時間情報を受信したとき、受信した実時間情報を復号化することで取得した放送実時間が、受信した視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、この期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可する。

【0020】このように、請求項1の発明によれば、放

送受信側は、送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、やはり送信側から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可するので、この結果、個別情報の量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送受信方法を得ることができる。

【0021】また、請求項2の発明は、映像、音声、又はデータ等を含む信号を放送する際に用いられる放送受信方法であって、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、放送受信側は、前記スクランブル信号及び前記視聴期限情報を受信したとき、当該受信したスクランブル信号及び視聴期限情報を蓄積しておき、当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、前記蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、当該期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを要旨とする。

【0022】請求項2の発明によれば、まず、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送する。

【0023】一方、放送受信側は、スクランブル信号及び視聴期限情報を受信したとき、受信したスクランブル信号及び視聴期限情報を蓄積しておき、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、この期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄

積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。このように、請求項2の発明によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信方法を得ることができる。

【0024】しかも、請求項3の発明は、映像、音声、又はデータ等を含む信号を放送する際に用いられる放送受信方法であって、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、放送受信側は、前記スクランブル信号及び前記視聴期限情報を受信したとき、当該受信したスクランブル信号及び視聴期限情報を蓄積しておき、当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、前記蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う一方、前記放送実時間のうち、今回と前回の放送実時間の間で時間的な連続性が失われているか否かに係る連続性判定を行い、前記期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下され、かつ、前記連続性判定の結果、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを要旨とする。

【0025】請求項3の発明によれば、まず、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、

特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送する。

【0026】一方、放送受信側は、スクランブル信号及び視聴期限情報を受信したとき、受信したスクランブル信号及び視聴期限情報を蓄積しておき、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、前記蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う一方、放送実時間のうち、今回と前回の放送実時間の間で時間的な連続性が失われているか否かに係る連続性判定を行い、期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下され、かつ、連続性判定の結果、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。このように、請求項3の発明によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、蓄積された特定の番組の視聴期限範囲内にある旨の判定が下され、かつ、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、請求項2の発明と同様に、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信方法を得ることができるのに加えて、さらに、例えば、蓄積されている特定の番組の再生視聴を、悪意をもって試みた盗人が、疑似的に暗号化した疑似実時間情報を、これを復号化する部分、例えばセキュリティモジュールに供与することで、目的とする特定の番組に何とかたどりつけたとしても、疑似的に暗号化した疑似実時間情報を時間的な連続性を保って供与し続けることは至難の技である結果として、きわめて高い耐タンパ性を持つ放送受信方法を得ることができる。

【0027】しかも、請求項4の発明は、映像、音声、又はデータ等を含む信号を放送する際に用いられる放送受信方法であって、放送送信側は、少なくとも、限定

受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、当該スクランブル信号の放送に先立って、個別情報に対して特定の基準値及び許容範囲を付加して放送する一方、前記スクランブル信号の放送に伴って、共通情報中の番組情報に対して前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加して放送し、放送受信側は、前記個別情報に付加された特定の基準値及び許容範囲を受信したとき、当該受信した特定の基準値を基礎として、前記受信した許容範囲から求められる第2の特定回数だけ前記放送送信側と共通の再帰的関数を用いて順次再帰的に生成した値を全てプールするとともに、前記スクランブル信号及び前記最終生成値を受信したとき、当該受信したスクランブル信号又は最終生成値を蓄積しておき、当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、前記蓄積された最終生成値を基礎として前記再帰的関数を用いて再帰的に生成した1つの値と、前記プールしておいた全ての値とを順次比較することで、当該両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、前記特定の番組の再生視聴要求を生じる毎に、前記蓄積された最終生成値を、前記生成した1つの値に更新記憶し、前記一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを要旨とする。

【0028】請求項4の発明によれば、まず、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、スクランブル信号の放送に先立って、個別情報に対して特定の基準値及び許容範囲を付加して放送する一方、スクランブル信号の放送に伴って、共通情報中の番組情報に対して特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加して放送する。

【0029】一方、放送受信側は、初めに、個別情報に付加された特定の基準値及び許容範囲を受信したとき、受信した特定の基準値を基礎として、同様に受信した許容範囲から求められる第2の特定回数だけ放送送信側と共通の再帰的関数を用いて順次再帰的に生成した値を全てプールするとともに、スクランブル信号及び最終生成値を受信したとき、受信したスクランブル信号又は最終生成値を蓄積しておく。

【0030】次に、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたと

き、蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、プールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行うが、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶する。

【0031】そして、放送受信側は、一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。

【0032】このように、請求項4の発明によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、プールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の特定回数から第1の特定回数を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信方法を得ることができる。

【0033】さらにまた、請求項5の発明は、前記再帰的関数としては、一方向性のハッシュ関数が採用されることを要旨とする。

【0034】請求項5の発明によれば、再帰的関数としては、一方向性のハッシュ関数が採用される。

【0035】一方、請求項6の発明は、映像、音声、又はデータ等を含む信号を放送する放送送信装置であって、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加する視聴期限情報付加手段と、放送実時間を含む実時間情報を暗号化する実時間情報暗号化手段と、前記スクランブル手段で生成したスクランブル信号と、前記視聴期限情報付加手段で視聴期限情報が付加された番組情報と、前記実時間情報暗号化手段で暗号化された実時間情報と、を多重化する多重化手段と、を備え、前記多重化された放送信号を変調して放送することを要旨とする。

【0036】請求項6の発明によれば、まず、放送信号の送信準備として、スクランブル手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成し、視聴期限情報付加手段は、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加し、さらに、実時間情報暗号化手段は、放送実時間を含む実時間情報を暗号化する。そして、多重化手段は、スクランブル手段で生成したスクランブル信号と、視聴期限情報付加手段で視聴期限情報が付加された番組情報と、実時間情報暗号化手段で暗号化された実時間情報と、を多重化し、このようにして多重化された放送信号を交調して放送する。

【0037】このように、請求項6の発明によれば、特定の番組に係るスクランブル信号と、特定の番組の視聴期限情報が付加された番組情報と、暗号化された実時間情報と、が多重化された放送信号を交調して放送するので、したがって、この信号を受信した放送受信側は、受信したスクランブル信号に係る特定の番組を、ストリーム型又は蓄積型のうちのいずれか一方で視聴する際に、視聴時期を基準とした特定の番組の視聴許可判定を行うことが可能となる結果として、放送受信側で視聴時期を基準とした特定の番組の視聴許可判定を行う際に適した信号を送信することができる。

【0038】また、請求項7の発明は、映像、音声、又はデータ等を含む信号を放送する放送送信装置であって、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、個別情報に対して特定の基準値及び許容範囲を付加する特定基準情報付加手段と、共通情報中の番組情報に対し、前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加する最終生成値付加手段と、前記スクランブル手段で生成したスクランブル信号と、前記特定基準情報付加手段で特定の基準値及び許容範囲が付加された個別情報と、前記最終生成値付加手段で最終生成値が付加された番組情報と、を多重化する多重化手段と、を備え、前記多重化された放送信号を交調して放送する際に、前記個別情報は、前記スクランブル信号の放送に先立って放送される一方、前記最終生成値は、前記スクランブル信号の放送に伴って放送されることを要旨とする。請求項7の発明によれば、まず、放送信号の送信準備として、スクランブル手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成し、特定基準情報付加手段は、個別情報に対して特定の基準値及び許容範囲を付加し、さらに、最終生成値付加手段は、共通情報中の番組情報に対し、特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加する。

そして、多重化手段は、スクランブル手段で生成したスクランブル信号と、特定基準情報付加手段で特定の基準値及び許容範囲が付加された個別情報と、最終生成値付加手段で最終生成値が付加された番組情報と、を多重化し、このようにして多重化された放送信号を交調して放送する際に、個別情報は、スクランブル信号の放送に先立って放送される一方、最終生成値は、スクランブル信号の放送に伴って放送される。

【0039】このように、請求項7の発明によれば、特定の番組に係るスクランブル信号と、特定の基準値及び許容範囲が付加された番組情報と、最終生成値が付加された番組情報と、が多重化された放送信号を交調して放送するので、したがって、この信号を受信した放送受信側は、受信したスクランブル信号に係る特定の番組を蓄積型で視聴する際に、視聴回数を基準とした特定の番組の視聴許可判定を行うことが可能となる結果として、放送受信側で視聴回数を基準とした特定の番組の視聴許可判定を行う際に適した信号を送信することができる。

【0040】さらに、請求項8の発明は、前記再帰的関数としては、一方方向性のハッシュ関数が採用されることを要旨とする。

【0041】請求項8の発明によれば、再帰的関数としては、一方方向性のハッシュ関数が採用される。

【0042】一方、請求項9の発明は、映像、音声、又はデータ等を含む放送信号を受信する放送受信装置であって、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、前記特定の番組の視聴期限を含む視聴期限情報、及び暗号化された放送実時間を含む実時間情報が多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、当該分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記分離手段で取り出された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う期限判定手段と、当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記分離手段で取り出されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、を備え、前記デスクランブル手段は、前記スクランブル信号に対するデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を実時間で視聴するストリーム型視聴を許可することを要旨とする。

【0043】請求項9の発明によれば、まず、分離手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、特定の番組の視聴期限を含む視聴期限情報、及び暗号化された放送実時間を含む実時間情報が多重化された

放送信号を受信して復調するとともに、復調した放送信号から信号又は情報を各々分離して取り出す。次に、期限判定手段は、分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、分離手段で取り出された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う。そして、デスクランブル手段は、期限判定手段における期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、前記分離手段で取り出されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を実時間で視聴するストリーム型視聴を許可する。

【0044】このように、請求項9の発明によれば、放送送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、やはり放送送信側から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、放送送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可するので、この結果、個別情報の量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送受信装置を得ることができる。

【0045】また、請求項10の発明は、映像、音声、又はデータ等を含む放送信号を受信する放送受信装置であって、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、前記特定の番組の視聴期限を含む視聴期限情報、及び暗号化された放送実時間を含む実時間情報が多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、当該分離手段で取り出されたスクランブル信号及び視聴期限情報を蓄積する番組蓄積手段と、当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に前記分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記番組蓄積手段に蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う期限判定手段と、当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、を備え、前記デスクランブル手段は、前記スクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する

ことを要旨とする。

【0046】請求項10の発明によれば、まず、分離手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、特定の番組の視聴期限を含む視聴期限情報、及び暗号化された放送実時間を含む実時間情報が多重化された放送信号を受信して復調するとともに、復調した放送信号から信号又は情報を各々分離して取り出す。次に、番組蓄積手段は、分離手段で取り出されたスクランブル信号及び視聴期限情報を蓄積しておく。期限判定手段は、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、再生視聴要求時に分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、番組蓄積手段に蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う。そして、デスクランブル手段は、期限判定手段における期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。

【0047】このように、請求項10の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、番組蓄積手段に蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信装置を得ることができる。

【0048】さらに、請求項11の発明は、映像、音声、又はデータ等を含む放送信号を受信する放送受信装置であって、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、個別情報に付加された特定の基準値及び許容範囲、並びに共通情報中の番組情報に付加された前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値が多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、当該分離手段で取り出された特定の

基準値を基礎として、前記取り出された許容範囲から求められる第2の特定回数だけ前記再帰的関数を用いて順次再帰的に生成した値を全てプールする値プール手段と、前記分離手段で取り出されたスクランブル信号又は最終生成値を蓄積する番組蓄積手段と、当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、前記番組蓄積手段に蓄積された最終生成値を基礎として前記再帰的関数を用いて再帰的に生成した1つの値と、前記値プール手段にプールしておいた全ての値とを順次比較することで、当該両者間で一致する値が存在するか否かに係る一致判定を行う視聴権判定手段と、前記特定の番組の再生視聴要求を生じる毎に、前記番組蓄積手段に蓄積された最終生成値を、前記視聴権判定手段で今回生成した1つの値に更新記憶する最終生成値更新記憶手段と、当該視聴権判定手段における一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、を備え、前記デスクランブル手段は、前記スクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを要旨とする。

【0049】請求項11の発明によれば、まず、分離手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号に伴って、個別情報に付加された特定の基準値及び許容範囲、並びに共通情報中の番組情報に付加された特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値が多重化された放送信号を受信して復調するとともに、復調した放送信号から信号又は情報を各々分離して取り出す。これを受けて、値プール手段は、分離手段で取り出された特定の基準値を基礎として、同様に取り出された許容範囲から求められる第2の特定回数だけ再帰的関数を用いて順次再帰的に生成した値を全てプールする一方、番組蓄積手段は、分離手段で取り出されたスクランブル信号又は最終生成値を蓄積しておく。番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、視聴権判定手段は、番組蓄積手段に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、値プール手段にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行う。このとき、最終生成値更新記憶手段は、特定の番組の再生視聴要求を生じる毎に、番組蓄積手段に蓄積された最終生成値を、視聴権判定手段で今回生成した1つの値に更新記憶する。そして、デスクランブル手段は、視聴権判定手段における一致判定の結果、両者間で一致する値が存在する

旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。

【0050】このように、請求項11の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、番組蓄積手段に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、値プール手段にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の特定回数から第1の特定回数を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信装置を得ることができる。

【0051】さらにまた、請求項12の発明は、前記再帰的関数としては、一方向性のハッシュ関数が採用されることを要旨とする。

【0052】請求項11の発明によれば、再帰的関数としては、一方向性のハッシュ関数が採用される。

【0053】一方、請求項13の発明は、映像、音声、又はデータ等を含む信号を放送する放送送信装置と、当該放送送信装置から放送された信号を受信する放送受信装置とを含んで構成される放送受信システムであって、前記放送送信装置は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加する視聴期限情報付加手段と、放送実時間を含む実時間情報を暗号化する実時間情報暗号化手段と、前記スクランブル手段で生成したスクランブル信号と、前記視聴期限情報付加手段で視聴期限情報が付加された番組情報と、前記実時間情報暗号化手段で暗号化された実時間情報と、を多重化する多重化手段と、を備え、前記多重化された放送信号を変調して放送し、前記放送受信装置は、前記多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、当該分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記分離手段で取り出された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあ

るか否かに係る期限判定を行う期限判定手段と、当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記分離手段で取り出されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、を備え、前記デスクランブル手段は、前記スクランブル信号に対するデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を実時間で視聴するストリーム型視聴を許可することを要旨とする。

【0054】請求項13の発明によれば、放送送信装置に属する各機能手段において、下記に述べる処理が順次実行される。

【0055】すなわち、まず、放送信号の送信準備として、スクランブル手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成し、視聴期限情報付加手段は、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加し、さらに、実時間情報暗号化手段は、放送実時間を含む実時間情報を暗号化する。そして、多重化手段は、スクランブル手段で生成したスクランブル信号と、視聴期限情報付加手段で視聴期限情報が付加された番組情報と、実時間情報暗号化手段で暗号化された実時間情報と、を多重化し、このようにして多重化された放送信号を変調して放送する。

【0056】一方、放送受信装置に属する各機能手段において、下記に述べる処理が順次実行される。

【0057】すなわち、まず、分離手段は、多重化された放送信号を受信して復調するとともに、復調した放送信号から信号又は情報を各々分離して取り出す。次に、期限判定手段は、分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、分離手段で取り出された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う。そして、デスクランブル手段は、期限判定手段における期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、前記分離手段で取り出されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を実時間で視聴するストリーム型視聴を許可する。

【0058】このように、請求項13の発明によれば、放送送信装置から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、やはり放送送信装置から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、放送送信装置から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組

のストリーム型視聴を許可するので、この結果、個別情報の量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送受信システムを得ることができる。

【0059】また、請求項14の発明は、映像、音声、又はデータ等を含む信号を放送する放送送信装置と、当該放送送信装置から放送された信号を受信する放送受信装置とを含んで構成される放送受信システムであって、前記放送送信装置は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加する視聴期限情報付加手段と、放送実時間を含む実時間情報を暗号化する実時間情報暗号化手段と、前記スクランブル手段で生成したスクランブル信号と、前記視聴期限情報付加手段で視聴期限情報が付加された番組情報と、前記実時間情報暗号化手段で暗号化された実時間情報と、を多重化する多重化手段と、を備え、前記多重化された放送信号を変調して放送し、前記放送受信装置は、前記多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、当該分離手段で取り出されたスクランブル信号及び視聴期限情報を蓄積する番組蓄積手段と、当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に前記分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、前記番組蓄積手段に蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う期限判定手段と、当該期限判定手段における期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、を備え、前記デスクランブル手段は、前記スクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを要旨とする。

【0060】請求項14の発明によれば、放送送信装置に属する各機能手段において、下記に述べる処理が順次実行される。

【0061】すなわち、まず、放送信号の送信準備として、スクランブル手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成し、視聴期限情報付加手段は、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加し、さらに、実時間情報暗号化手段は、放送実時間を含む実時間情報を暗号化する。そ

して、多重化手段は、スクランブル手段で生成したスクランブル信号と、視聴期限情報付加手段で視聴期限情報が付加された番組情報と、実時間情報暗号化手段で暗号化された実時間情報と、を多重化し、このようにして多重化された放送信号を変調して放送する。

【0062】一方、放送受信装置に属する各機能手段において、下記に述べる処理が順次実行される。

【0063】すなわち、まず、分離手段は、多重化された放送信号を受信して復調するとともに、復調した放送信号から信号又は情報を各々分離して取り出す。次に、番組蓄積手段は、分離手段で取り出されたスクランブル信号及び視聴期限情報を蓄積しておく。期限判定手段は、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、再生視聴要求時に分離手段で取り出された実時間情報を復号化することで取得した放送実時間が、番組蓄積手段に蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う。そして、デスクランブル手段は、期限判定手段における期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。

【0064】このように、請求項14の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に放送送信装置から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、番組蓄積手段に蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信システムを得ることができる。

【0065】さらに、請求項15の発明は、映像、音声、又はデータ等を含む信号を放送する放送送信装置と、当該放送送信装置から放送された信号を受信する放送受信装置とを含んで構成される放送受信システムであって、前記放送送信装置は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成するスクランブル手段と、個別情報に対して特定の基準値及び許容範囲を付加する

特定基準情報付加手段と、共通情報中の番組情報に対し、前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加する最終生成値付加手段と、前記スクランブル手段で生成したスクランブル信号と、前記特定基準情報付加手段で特定の基準値及び許容範囲が付加された個別情報と、前記最終生成値付加手段で最終生成値が付加された番組情報と、を多重化する多重化手段と、を備え、前記多重化された放送信号を変調して放送する際に、前記個別情報は、前記スクランブル信号の放送に先立って放送される一方、前記最終生成値は、前記スクランブル信号の放送に伴って放送され、前記放送受信装置は、前記多重化された放送信号を受信して復調するとともに、当該復調した放送信号から信号又は情報を各々分離して取り出す分離手段と、当該分離手段で取り出された特定の基準値を基礎として、前記取り出された許容範囲から求められる第2の特定回数だけ前記放送送信装置と共通の再帰的関数を用いて順次再帰的に生成した値を全てプールする値プール手段と、前記分離手段で取り出されたスクランブル信号又は最終生成値を蓄積する番組蓄積手段と、当該番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、前記番組蓄積手段に蓄積された最終生成値を基礎として前記再帰的関数を用いて再帰的に生成した1つの値と、前記値プール手段にプールしておいた全ての値とを順次比較することで、当該両者間で一致する値が存在するか否かに係る一致判定を行う視聴権判定手段と、前記特定の番組の再生視聴要求を生じる毎に、前記番組蓄積手段に蓄積された最終生成値を、前記視聴権判定手段で今回生成した1つの値に更新記憶する最終生成値更新記憶手段と、当該視聴権判定手段における一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すデスクランブル手段と、を備え、前記デスクランブル手段は、前記スクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを要旨とする。

【0066】請求項15の発明によれば、放送送信装置に属する各機能手段において、下記に述べる処理が順次実行される。

【0067】すなわち、まず、放送信号の送信準備として、スクランブル手段は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成し、特定基準情報付加手段は、個別情報に対して特定の基準値及び許容範囲を付加し、さらに、最終生成値付加手段は、共通情報中の番組情報に対し、特定の基準値を基礎として第1の特定回数だけ

再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加する。そして、多重化手段は、スクランブル手段で生成したスクランブル信号と、特定基準情報付加手段で特定の基準値及び許容範囲が付加された個別情報と、最終生成値付加手段で最終生成値が付加された番組情報と、を多重化し、このようにして多重化された放送信号を変調して放送する際に、個別情報は、スクランブル信号の放送に先立って放送される一方、最終生成値は、スクランブル信号の放送に伴って放送される。

【0068】一方、放送受信装置に属する各機能手段において、下記に述べる処理が順次実行される。

【0069】すなわち、まず、分離手段は、多重化された放送信号を受信して復調するとともに、復調した放送信号から信号又は情報を各々分離して取り出す。これを受けて、値プールの手段は、分離手段で取り出された特定の基準値を基礎として、同様に取り出された許容範囲から求められる第2の特定回数だけ再帰的関数を用いて順次再帰的に生成した値を全てプールする一方、番組蓄積手段は、分離手段で取り出されたスクランブル信号又は最終生成値を蓄積しておく。番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、視聴権判定手段は、番組蓄積手段に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、値プール手段にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行う。このとき、最終生成値更新記憶手段は、特定の番組の再生視聴要求を生じる毎に、番組蓄積手段に蓄積された最終生成値を、視聴権判定手段で今回生成した1つの値に更新記憶する。そして、デスクランブル手段は、視聴権判定手段における一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。

【0070】このように、請求項15の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、番組蓄積手段に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、値プール手段にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許

可するので、したがって、第2の特定回数から第1の特定回数を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信システムを得ることができる。

【0071】そして、請求項16の発明は、前記再帰的関数としては、一方向性のハッシュ関数が採用されることを要旨とする。

【0072】請求項16の発明によれば、再帰的関数としては、一方向性のハッシュ関数が採用される。

【0073】

【発明の実施の形態】以下に、本発明に係る放送受信方法、放送送信装置、放送受信装置、及び放送受信システムの各実施形態について、図に基づいて詳細に説明する。

【0074】図1(a)は、本発明に係る第1乃至第2の放送受信方法が適用される、第1乃至第2の放送送信装置の機能ブロック構成図、図1(b)は、本発明に係る第1乃至第2の放送受信方法が適用される、第1乃至第2の放送受信装置の機能ブロック構成図、図2(a)は、本発明に係る第3の放送受信方法が適用される、第3の放送送信装置の機能ブロック構成図、図2(b)は、本発明に係る第3の放送受信方法が適用される、第3の放送受信装置の機能ブロック構成図である。

【0075】まず、本発明に係る第1の放送受信方法の概略について述べると、本第1の放送受信方法は、映像、音声、又はデータ等を含む信号を放送する際に用いられるものであり、受信した番組を実時間で視聴するストリーム型視聴を行う場合に適用される。

【0076】詳しく述べると、本第1の放送受信方法では、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、放送受信側は、前記スクランブル信号、前記視聴期限情報、及び前記実時間情報を受信したとき、当該受信した実時間情報を復号化することで取得した放送実時間が、前記受信した視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、当該期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記受信したスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を実時間で視聴するストリーム型視聴を許可することを特徴としている。

【0077】本第1の放送受信方法によれば、放送受信側は、送信側から暗号化されて放送された実時間情報

を復号化することで取得した放送実時間が、やはり送信側から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可するので、この結果、個別情報の量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送送受信方法を得ることができる。

【0078】次に、本発明に係る第2の放送送受信方法の概略について述べると、本第2の放送送受信方法は、映像、音声、又はデータ等を含む信号を放送する際に用いられるものであり、受信した番組を蓄積後に視聴する蓄積型視聴を行う場合に適用される。

【0079】詳しく述べると、本第2の放送送受信方法では、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、放送受信側は、前記スクランブル信号及び前記視聴期限情報を受信したとき、当該受信したスクランブル信号及び視聴期限情報を蓄積しておき、当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、前記蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行い、当該期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴としている。

【0080】本第2の放送送受信方法によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の

意図に反した番組視聴を可及的に抑制可能な放送送受信方法を得ることができる。

【0081】また、上述した第2の放送送受信方法の一部をさらに改良した放送送受信方法では、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、共通情報中の番組情報に対し、前記特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送し、放送受信側は、前記スクランブル信号及び前記視聴期限情報を受信したとき、当該受信したスクランブル信号及び視聴期限情報を蓄積しておき、当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、当該再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、前記蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う一方、前記放送実時間のうち、今回と前回の放送実時間の間で時間的な連続性が失われているか否かに係る連続性判定を行い、前記期限判定の結果、前記放送実時間が前記視聴期限範囲内にある旨の判定が下され、かつ、前記連続性判定の結果、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴としている。

【0082】第2の放送送受信方法の一部をさらに改良した放送送受信方法によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、蓄積された特定の番組の視聴期限範囲内にある旨の判定が下され、かつ、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の放送送受信方法と同様に、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送送受信方法を得ることができるのに加えて、さらに、例えば、蓄積されている特定の番組の再生視聴を、悪意をもって試みた盗人が、擬似的に暗号化した疑似実時間情報を、これを復号化する部分、例えばセキュリティモジュ

ールに供与することで、目的とする特定の番組になんとかたどりつけたとしても、擬似的に暗号化した疑似実時間情報を時間的な連続性を保って供与し続けることは至難の技である結果として、きわめて高い耐タンパ性を持つ放送送受信方法を得ることができる。

【0083】そして、本発明に係る第3の放送送受信方法の概略について述べると、本第3の放送送受信方法は、映像、音声、又はデータ等を含む信号を放送する際に用いられるものであり、受信した番組を蓄積後に視聴する蓄積型視聴を行う場合に適用される。

【0084】詳しく述べると、本第3の放送送受信方法では、放送送信側は、少なくとも、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施したスクランブル信号を放送する際に、当該スクランブル信号の放送に先立って、個別情報に対して特定の基準値及び許容範囲を付加して放送する一方、前記スクランブル信号の放送に伴って、共通情報中の番組情報に対して前記特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加して放送し、放送受信側は、前記個別情報に付加された特定の基準値及び許容範囲を受信したとき、当該受信した特定の基準値を基礎として、前記受信した許容範囲から求められる第2の特定回数だけ前記放送送信側と共通の再帰的関数を用いて順次再帰的に生成した値を全てプールするとともに、前記スクランブル信号及び前記最終生成値を受信したとき、当該受信したスクランブル信号又は最終生成値を蓄積しておき、当該蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、前記蓄積された最終生成値を基礎として前記再帰的関数を用いて再帰的に生成した1つの値と、前記プールしておいた全ての値とを順次比較することで、当該両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、前記特定の番組の再生視聴要求を生じる毎に、前記蓄積された最終生成値を、前記生成した1つの値に更新記憶し、前記一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、前記特定の番組に係る視聴権が存在するとみなして、前記蓄積されたスクランブル信号に対してデスクランブル処理を施すことで前記特定の番組に係る原信号を復元することにより、当該特定の番組を蓄積後に再生視聴する蓄積型視聴を許可することを特徴としている。

【0085】本第3の放送送受信方法によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、プールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致す

る値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の特定回数から第1の特定回数を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送送受信方法を得ることができる。

【0086】なお、第3の放送送受信方法の変形例として、上述した再帰的関数としては、一方向性のハッシュ関数を採用することができる。

【0087】次に、上述した第1乃至第2の放送送受信方法が適用される第1乃至第2の放送送信装置、第1乃至第2の放送受信装置、及び第1乃至第2の放送送受信システムについて、以下に詳細に説明する。

【0088】図1は、第1乃至第2の放送送受信方法が適用される、第1乃至第2の放送送信装置13、及び第1乃至第2の放送受信装置15を含んで構成される第1乃至第2の放送送受信システム11の機能ブロック構成を表している。なお、第1乃至第2の放送送受信システム11は、その構成が両者間で共通であるため、1つの実施形態を説明することで、両者の説明に代えることとする。

【0089】初めに、第1乃至第2の放送送信装置13の構成について説明すると、第1乃至第2の放送送信装置13は、スクランブル手段として機能するスクランブル部21と、視聴期限情報付加手段及び実時間情報暗号化手段として機能する第1の暗号部23と、暗号化された個別情報を解読する際に用いられるマスタ鍵Kmを管理するKm管理部25と、第2の暗号部27と、多重化手段として機能する多重部29と、を備えて構成されている。

【0090】スクランブル部21は、限定受信対象となる特定の番組に係る原信号に対してスクランブル鍵Ksを用いたスクランブル処理を施すことでスクランブル信号を生成するスクランブル機能を有している。

【0091】第1の暗号部23は、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加する視聴期限情報付加機能と、放送実時間を含む実時間情報を暗号化する実時間情報暗号化機能と、を有しており、第1の暗号部23において、視聴期限情報、実時間情報、及びスクランブル鍵Ksが、ワーク鍵Kwを用いて暗号化される。

【0092】第2の暗号部27は、Km管理部25で管理されているマスタ鍵Kmを用いて個別情報を暗号化する機能を有している。

【0093】そして、多重部29は、スクランブル部21で生成したスクランブル信号と、第1の暗号部23で

暗号化された、番組情報、実時間情報、及びスクランブル鍵Ksを含む情報と、第2の暗号部27で暗号化された、個別情報、及びワーク鍵Kwを含む情報とを、例えばMPEG-2 SYSTEMSで規定されているパケット多重方式を用いて多重化する多重化機能を有して構成されている。なお、多重部29で多重化された放送信号は、例えばQPSKなどを用いて変調して放送される。

【0094】一方、第1乃至第2の放送受信装置15の構成について説明すると、第1乃至第2の放送受信装置15は、分離手段として機能する分離部31と、番組蓄積手段として機能する番組蓄積管理部33と、切替器35と、期限判定手段を含む第1のセキュリティモジュール37と、デスクランブル手段として機能するデスクランブル部39と、を備えて構成されている。

【0095】分離部31は、多重部29で多重化された放送信号を受信して復調するとともに、復調した放送信号からスクランブル信号又は各種情報を各々分離して取り出す機能を有している。

【0096】番組蓄積管理部33は、分離部31で取り出されたスクランブル信号及び番組情報を蓄積する番組蓄積機能を有しており、分離部31で取り出されたスクランブル信号及び番組情報の蓄積制御を行う蓄積制御部41と、スクランブル信号に係る特定の番組をスクランブル状態を維持して蓄積する番組蓄積部43と、視聴期限情報を含む番組情報を蓄積する番組情報蓄積部45と、番組蓄積部43に蓄積されたスクランブル信号、又は番組情報蓄積部45に蓄積された番組情報の出力制御を行う出力制御部47と、を備えて構成されている。

【0097】切替器35は、分離部31で分離して取り出されたスクランブル信号及び番組情報と、出力制御部47から出力される、番組蓄積管理部33に一旦蓄積されたスクランブル信号及び番組情報とのうち、いずれか一方を選択的に切替え出力する切替機能を有している。

【0098】第1のセキュリティモジュール37は、番組蓄積管理部33に一旦蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、番組蓄積管理部33に蓄積された番組情報中の視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行う期限判定機能と、時々刻々と変化する放送実時間のうち、今回と前回の放送実時間の間で時間的な連続性が保たれているか否かに係る連続性判定を行う連続性判定機能と、期限判定機能を発揮することで得られた期限判定結果を主として、連続性判定機能を発揮することで得られた連続性判定結果を必要に応じて加味して、特定の番組に係る視聴権が存在するか否かに係る視聴権判定を行う視聴権判定機能と、を有している。

【0099】なお、第1のセキュリティモジュール37

は、第1の復号部51と、個別情報を復号化する際に用いられるマスタ鍵Kmを管理するKm管理部53と、第2の復号部55と、番組情報管理部57と、個別情報管理部59と、視聴権判定部61と、Ks出力制御部63と、を含んで構成されている。

【0100】第2の復号部55は、分離部31で分離して取り出された個別情報を、Km管理部53が管理しているマスタ鍵Kmを用いて復号化する機能を有している。第2の復号部55で復号化された個別情報は、個別情報管理部59に送出されて記憶管理される。

【0101】第1の復号部51は、切替器35の出力である視聴期限情報を含む番組情報と、分離部31で分離して取り出された実時間情報とを、個別情報管理部59で記憶管理されている個別情報中のワーク鍵Kwを用いて復号化する機能を有している。第1の復号部51で復号化された番組情報及び放送実時間は、番組情報管理部57に送出されて記憶管理される。

【0102】なお、番組情報管理部57は、時々刻々と変化する放送実時間のうち、最新のタイミングで受信した今回の放送実時間と、直前のタイミングで受信した前回の放送実時間とを常時更新しつつ記憶管理するとともに、今回と前回の放送実時間の間での時間的な連続性が保たれているか否かに係る連続性判定を行い、この連続性判定結果を視聴権判定部61宛に伝える機能を有している。

【0103】視聴権判定部61は、番組蓄積管理部33に一旦蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、番組蓄積管理部33に蓄積された番組情報中の視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行うとともに、この期限判定結果を主として、さらに、番組情報管理部57から送られてきた連続性判定結果を必要に応じて加味して、特定の番組に係る視聴権が存在するか否かに係る視聴権判定を行う視聴権判定機能を有している。具体的には、視聴権判定部61は、放送実時間が特定の番組の視聴期限範囲内にある旨の判定が下されたとき、又は、放送実時間が特定の番組の視聴期限範囲内にある旨の判定が下され、かつ、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、特定の番組に係る視聴権が存在する旨の判定を下すように構成されている。

【0104】なお、放送実時間が特定の番組の視聴期限範囲内にある旨の判定が下され、かつ、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、特定の番組に係る視聴権が存在する旨の判定を下すように視聴権判定部61を構成した場合には、例えば、蓄積されている特定の番組の再生視聴を、悪意をもって試みた盗人が、擬似的に暗号化

した疑似実時間情報を、これを復号化する部分、すなわちセキュリティモジュール37に供与することで、目的とする特定の番組になんとかたどりつけたとしても、疑似的に暗号化した疑似実時間情報を時間的な連続性を保って供与し続けることは至難の技である結果として、きわめて高い耐タンパ性を持つ放送受信装置、並びに放送受信システムを得ることができる。

【0105】さらに、Ks出力制御部63は、視聴権判定部61において特定の番組に係る視聴権が存在する旨の判定が下されたとき、視聴権判定部61からの指示に基づき、特定の番組に係るスクランブル信号に対してデスクランブル処理を行う際に用いられるスクランブル鍵Ksの出力制御を行う鍵出力制御機能を有して構成されている。

【0106】そして、デスクランブル部39は、Ks出力制御部63からのスクランブル鍵Ksの出力を受けて、特定の番組に係るスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元するデスクランブル機能を有しており、これにより、特定の番組を実時間で視聴するストリーム型視聴を許可するか、又は特定の番組を蓄積後に再生視聴する蓄積型視聴を許可するように構成されている。

【0107】次に、上述のように構成された第1乃至第2の放送送受信システム11の動作について、ストリーム型視聴を行う場合と、蓄積型視聴を行う場合とに分けて説明する。

【0108】まず、ストリーム型視聴を行う場合の第1乃至第2の放送送受信システム11の動作について説明すると、放送送信装置13に属する各機能部において、下記に述べる処理が順次実行される。

【0109】すなわち、まず、放送信号の送信準備として、スクランブル部21は、限定受信対象となる特定の番組に係る原信号に対してスクランブル鍵Ksを用いたスクランブル処理を施すことでスクランブル信号を生成し、第1の暗号部23は、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加し、さらに、放送実時間を含む実時間情報を暗号化する。そして、多重部29は、スクランブル部21で生成したスクランブル信号と、第1の暗号部23で視聴期限情報が付加された番組情報、及び暗号化された実時間情報と、を多重化し、このようにして多重化された放送信号が変調して放送される。なお、視聴期限情報が付加された番組情報を暗号化してスクランブル信号に併せて放送する形態を採用することもできる。

【0110】一方、放送受信装置15に属する各機能部において、下記に述べる処理が順次実行される。

【0111】すなわち、まず、分離部31は、多重化された放送信号を受信して復調するとともに、復調した放送信号からスクランブル信号又は各種情報を各々分離して取り出す。次に、視聴権判定部61は、分離部31で

取り出された実時間情報を復号化することで取得した放送実時間が、分離部31で取り出された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行うことで、放送受信装置15自身が正当な視聴権を有するか否かを判定する。そして、デスクランブル部39は、視聴権判定部61における期限判定の結果、放送実時間が視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、分離部31で取り出されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を実時間で視聴するストリーム型視聴を許可する。

【0112】このように、第1乃至第2の放送送受信システム11によれば、放送送信装置13から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、やはり放送送信装置13から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、放送送信装置13から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可するので、この結果、個別情報の量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送送受信システムを得ることができる。

【0113】次に、蓄積型視聴を行う場合の第1乃至第2の放送送受信システム11の動作について説明すると、放送送信装置13に属する各機能部において、下記に述べる処理が順次実行される。

【0114】すなわち、まず、放送信号の送信準備として、スクランブル部21は、限定受信対象となる特定の番組に係る原信号に対してスクランブル鍵Ksを用いたスクランブル処理を施すことでスクランブル信号を生成し、第1の暗号部23は、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加し、さらに、放送実時間を含む実時間情報を暗号化する。そして、多重部29は、スクランブル部21で生成したスクランブル信号と、第1の暗号部23で視聴期限情報が付加された番組情報、及び暗号化された実時間情報と、を多重化し、このようにして多重化された放送信号が変調して放送される。なお、視聴期限情報が付加された番組情報を暗号化してスクランブル信号に併せて放送する形態を採用することもできる。

【0115】一方、放送受信装置15に属する各機能部において、下記に述べる処理が順次実行される。

【0116】すなわち、まず、分離部31は、多重化された放送信号を受信して復調するとともに、復調した放送信号からスクランブル信号又は各種情報を各々分離して取り出す。次に、番組蓄積管理部33は、分離部31で取り出されたスクランブル信号及び視聴期限情報を蓄

積しておく。視聴権判定部61は、番組蓄積管理部33に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、再生視聴要求時に分離部31で取り出された実時間情報を復号化することで取得した放送実時間が、番組蓄積管理部33に蓄積された視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行うとともに、この期限判定結果を主として、さらに、番組情報管理部57から送られてきた連続性判定結果を必要に応じて加味して、特定の番組に係る視聴権が存在するか否かを判定する。そして、デスクランブル部39は、視聴権判定部61における視聴権判定の結果、放送実時間が特定の番組の視聴期限範囲内にある旨の判定が下されるか、又は、放送実時間が特定の番組の視聴期限範囲内にある旨の判定が下され、かつ、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、特定の番組に係る視聴権が存在するとみなして、番組蓄積管理部33に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。

【0117】このように、第1乃至第2の放送送受信システム11によれば、番組蓄積管理部33に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に放送送信装置13から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、番組蓄積管理部33に蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、番組蓄積管理部33に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送送受信システムを得ることができる。

【0118】しかも、さらに改良された第1乃至第2の放送送受信システム11によれば、放送実時間が番組蓄積管理部33に蓄積された特定の番組の視聴期限範囲内にある旨の判定が下され、かつ、今回と前回の放送実時間の間で時間的な連続性が失われていない旨の判定が下されたときに初めて、特定の番組に係る視聴権が存在するとみなして、番組蓄積管理部33に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで、特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視

聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送送受信システムを得ることができるのに加えて、さらに、例えば、蓄積されている特定の番組の再生視聴を、悪意をもって試みた盗人が、擬似的に暗号化した疑似実時間情報を、これを復号化する部分、例えばセキュリティモジュールに供与することで、目的とする特定の番組に何とかたどりつけたとしても、擬似的に暗号化した疑似実時間情報を時間的な連続性を保って供与し続けることは至難の技である結果として、きわめて高い耐タンパ性を持つ放送送受信システムを得ることができる。

【0119】次に、上述した第3の放送送受信方法が適用される第3の放送送信装置、第3の放送受信装置、及び第3の放送送受信システムについて以下に説明する。

【0120】図2は、第3の放送送受信方法が適用される、第3の放送送信装置103、及び第3の放送受信装置105を含んで構成される第3の放送送受信システム101の機能ブロック構成を表している。なお、第3の放送送受信システム101は、第1乃至第2の放送送受信システム11との間で共通する構成部分を含んでいるため、両者間で共通する構成部分には同一の符号を付してその説明を省略し、両者間で相違する構成部分を中心に説明する。

【0121】初めに、第3の放送送信装置103の構成について説明すると、第1乃至第2の放送送信装置13では、スクランブル信号を放送する際に、共通情報中の番組情報に対し、特定の番組の視聴期限を含む視聴期限情報を付加して放送するとともに、放送実時間を含む実時間情報を暗号化して放送していたのに対し、第3の放送送信装置103では、スクランブル信号を放送する際に、スクランブル信号の放送に先立って、個別情報に対して特定の基準値B及び許容範囲nを付加して放送する一方、スクランブル信号の放送に伴って、共通情報中の番組情報に対して特定の基準値を基礎として第1の特定回数だけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加して放送するようにしている。

【0122】このため、第3の放送送信装置103は、最終生成値付加手段として機能する数値生成部111を有しており、この数値生成部111において、特定の基準値を基礎として第1の特定回数mだけ再帰的関数を用いて順次再帰的に値が生成され、生成した値のうちの最終生成値が、共通情報中の番組情報に対して付加されるように構成されている。

【0123】次に、第3の放送受信装置105の構成について説明すると、第1乃至第2の放送送信装置13では、例えば蓄積型視聴を行う場合には、第1のセキュリティモジュール37は、番組蓄積管理部33に一旦蓄積されたスクランブル信号に係る特定の番組の再生視聴要

求を生じたとき、再生視聴要求時に受信した実時間情報を復号化することで取得した放送実時間が、番組蓄積管理部33に蓄積された番組情報中の視聴期限情報に含まれる特定の番組の視聴期限範囲内にあるか否かに係る期限判定を行うことで、特定の番組に係る視聴権が存在するか否かに係る視聴権判定を行い、視聴権判定部61において特定の番組に係る視聴権が存在する旨の判定が下されたとき、視聴権判定部61からの指示に基づき、特定の番組に係るスクランブル信号に対してデスクランブル処理を行う際に用いられるスクランブル鍵Ksの出力制御を行うのに対し、第2のセキュリティモジュール113は、番組蓄積管理部33に一旦蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、番組情報管理部57に蓄積された最終生成値を基礎として送信側と共通の再帰的関数を用いて再帰的に生成した1つの値と、受信した特定の基準値Bを基礎として、受信した許容範囲nから求められる第2の特定回数nだけ放送送信側と共通の再帰的関数を用いて順次再帰的に生成してプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、前記一致判定の結果、前記両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、番組蓄積管理部33に蓄積されたスクランブル信号に対してデスクランブル処理を行う際に用いられるスクランブル鍵Ksの出力制御を行うようにしている。

【0124】このため、第3の放送受信装置105は、数値生成部115と、値プール手段として機能する数値プール部117と、を有しており、数値生成部115において、特定の基準値Bを基礎として、許容範囲nから求められる第2の特定回数nだけ放送送信側と共通の再帰的関数を用いて順次再帰的に値が生成され、生成した複数の値が数値プール部117にプールされるように構成されている。

【0125】次に、上述のように構成された第3の放送受信システム101の動作について説明すると、放送送信装置103に属する各機能部において、下記に述べる処理が順次実行される。

【0126】すなわち、まず、放送信号の送信準備として、スクランブル部21は、限定受信対象となる特定の番組に係る原信号に対してスクランブル処理を施すことでスクランブル信号を生成し、第1の又は第2の暗号部23、27は、個別情報に対して特定の基準値B及び許容範囲nを付加して暗号化し、さらに、共通情報中の番組情報に対し、特定の基準値を基礎として第1の特定回数mだけ再帰的関数を用いて順次再帰的に生成した値のうちの最終生成値を付加して暗号化する。そして、多重化部29は、スクランブル部21で生成したスクラン

ブル信号と、各自が暗号化されている、特定の基準値B及び許容範囲nが付加された個別情報と、最終生成値が付加された番組情報と、を多重化し、このようにして多重化された放送信号が変調して放送される。この際に、個別情報は、スクランブル信号の放送に先立って放送される一方、最終生成値は、スクランブル信号の放送に伴って放送される。

【0127】一方、放送受信装置105に属する各機能部において、下記に述べる処理が順次実行される。

【0128】すなわち、まず、分離部31は、多重化された放送信号を受信して復調するとともに、復調した放送信号からスクランブル信号又は各種情報を各々分離して取り出す。これを受けて、数値生成部115は、分離部31で取り出された特定の基準値Bを基礎として、同様に取り出された許容範囲nから求められる第2の特定回数nだけ再帰的関数を用いて順次再帰的に数値を生成し、生成した値を数値プール部117に全てプールする一方、番組蓄積管理部33は、分離部31で取り出されたスクランブル信号又は最終生成値を蓄積する一方で、番組情報管理部57は、最終生成値を蓄積しておく。番組蓄積管理部33に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、視聴権判定部61は、番組情報管理部57に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、数値プール部117にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行う。このとき、最終生成値更新記憶手段として機能する番組情報管理部57は、特定の番組の再生視聴要求を生じる毎に、番組蓄積管理部33に蓄積された最終生成値を、視聴権判定部61で今回生成した1つの値に更新記憶する。そして、デスクランブル部39は、視聴権判定部61における一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、番組蓄積管理部33に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組を蓄積後に再生視聴する蓄積型視聴を許可する。

【0129】上述した動作をさらにわかりやすくするために、契約視聴者が特定の番組を蓄積型で再生視聴する際において、蓄積型再生視聴の回数を制限する形態を例示して説明する。具体的には、蓄積した日付つまり放送日から、蓄積型再生視聴回数を例えば15回に限定する形態を例示して説明する。

【0130】まず、放送送信装置103側では、スクランブル信号の放送に伴って、以下の情報を放送する。すなわち、特定の基準値B及び許容範囲n ($n=30$) を、個別情報に付加して放送する。さらに、特定の基準値B ($B=0$) を基礎として第1の特定回数m ($m=15$) だけ再帰的関数を用いて順次再帰的に生成した値の

うちの最終生成値B15を、共通情報中の番組情報に付加して放送する。

【0131】放送受信装置105側では、個別情報を受信したとき、個別情報中の特定の基準値Bを基礎として、許容範囲 n ($n=30$) から求められる第2の特定回数 n ($n=30$) だけ送信側と同様の再帰的関数を用いて順次再帰的に生成した値(B1~B30)を数値プール部117にプールしておく。また、特定の番組に係るスクランブル信号及び番組情報を受信したとき、スクランブル信号又は番組情報に含まれる最終生成値B15を、番組蓄積管理部33に蓄積する一方で、番組情報管理部57は、番組情報に含まれる最終生成値B15を蓄積しておく。視聴契約者が特定の番組を初めて視聴しようとした場合には、番組情報管理部57に蓄積されている最終生成値B15を基礎として再帰的関数を用いて再帰的に生成した1つの値B16と、数値プール部117にプールしておいた全ての値(B1~B30)とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行う。この場合、1つの値B16は、数値プール部117にプールしておいた全ての値(B1~B30)のなかに一致する値が存在するので、蓄積型視聴を許可する。このとき、番組情報管理部57は、特定の番組の再生視聴要求を生じる毎に、番組蓄積管理部33に蓄積された最終生成値を、視聴権判定部61で今回生成した1つの値B16に更新記憶する。以上の処理を順次繰り返すことにより、第2の特定回数 n ($n=30$) から第1の特定回数 m ($m=15$) を減算することで得られた回数($n-m=15$) 制限下で蓄積型視聴が許可されることになる。

【0132】このように、第3の放送送受信システム101によれば、番組蓄積管理部33に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、番組情報管理部57に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、数値プール部117にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の特定回数 n から第1の特定回数 m を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送送受信システムを得ることができる。

【0133】なお、本発明は、上述した実施形態の例に

限定されることなく、請求の範囲内において適宜の変更を加えることにより、その他の態様で実施することが可能である。

【0134】すなわち、例えば、本発明で言う限定受信対象となる特定の番組として、例えば映像、音声、又はデータを含む形態を例示して説明したが、本発明はこの形態のみに限定されることなく、制御データやアプリケーションデータ、図形、写真、その他のあらゆる形態の情報を含む番組を限定受信対象として取り扱うことが可能であることは言うまでもない。

【0135】

【発明の効果】請求項1の発明によれば、放送受信側は、送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、やはり送信側から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可するので、この結果、個別情報の量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送送受信方法を得ることができる。

【0136】また、請求項2の発明によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送送受信方法を得ることができる。

【0137】さらに、請求項3の発明によれば、請求項2の発明と同様に、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送送受信方法を得ることができるのに加えて、さらに、例えば、蓄積されている特定の番組の再生視聴を、悪意をもって試みた盗人が、擬似的に暗号化した疑似実時間情報を、これを復号化する部分、例えばセキュリティモジュールに供与することで、目的とする特定の番組

になんとかたどりつけたとしても、擬似的に暗号化した疑似実時間情報を時間的な連続性を保って供与し続けることは至難の技である結果として、きわめて高い耐タンパ性を持つ放送受信方法を得ることができる。

【0138】しかも、請求項4の発明によれば、放送受信側は、蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、プールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の特定回数から第1の特定回数を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信方法を得ることができる。

【0139】一方、請求項6の発明によれば、特定の番組に係るスクランブル信号と、特定の番組の視聴期限情報が付加された番組情報と、暗号化された実時間情報と、が多重化された放送信号を変調して放送するので、したがって、この信号を受信した放送受信側は、受信したスクランブル信号に係る特定の番組を、ストリーム型又は蓄積型のうちのいずれか一方で視聴する際に、視聴時期を基準とした特定の番組の視聴許可判定を行うことが可能となる結果として、放送受信側で視聴時期を基準とした特定の番組の視聴許可判定を行う際に適した信号を送信することができる。

【0140】また、請求項7の発明によれば、特定の番組に係るスクランブル信号と、特定の基準値及び許容範囲が付加された番組情報と、最終生成値が付加された番組情報と、が多重化された放送信号を変調して放送するので、したがって、この信号を受信した放送受信側は、受信したスクランブル信号に係る特定の番組を蓄積型で視聴する際に、視聴回数を基準とした特定の番組の視聴許可判定を行うことが可能となる結果として、放送受信側で視聴回数を基準とした特定の番組の視聴許可判定を行う際に適した信号を送信することができる。

【0141】一方、請求項9の発明によれば、放送送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、やはり放送送信側から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、放送送信側から受信したスクランブル信号に対

してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可するので、この結果、個別情報の量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送受信装置を得ることができる。

【0142】また、請求項10の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に送信側から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、番組蓄積手段に蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、送信側から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信装置を得ることができる。

【0143】さらに、請求項11の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、番組蓄積手段に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、値プール手段にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の特定回数から第1の特定回数を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信装置を得ることができる。

【0144】一方、請求項13の発明によれば、放送送信装置から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、やはり放送送信装置から放送された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、放送送信装置から受信したスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組のストリーム型視聴を許可するので、この結果、個別情報の

量を増大させることなく、個々の番組毎に視聴時期を基準とした視聴期限を設定可能な放送受信システムを得ることができる。

【0145】また、請求項14の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、この再生視聴要求時に放送送信装置から暗号化されて放送された実時間情報を復号化することで取得した放送実時間が、番組蓄積手段に蓄積された特定の番組の視聴期限範囲内にある旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、番組蓄積手段に蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、特定の番組を蓄積した時点は視聴期限範囲内にあるが、再生視聴要求時点は視聴期限の範囲外にある場合には、特定の番組の蓄積型視聴が許可されない結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信システムを得ることができる。

【0146】さらに、請求項15の発明によれば、番組蓄積手段に蓄積されたスクランブル信号に係る特定の番組の再生視聴要求を生じたとき、番組蓄積手段に蓄積された最終生成値を基礎として再帰的関数を用いて再帰的に生成した1つの値と、値プール手段にプールしておいた全ての値とを順次比較することで、両者間で一致する値が存在するか否かに係る一致判定を行い、このとき、特定の番組の再生視聴要求を生じる毎に、蓄積された最終生成値を、今回生成した1つの値に更新記憶し、上記一致判定の結果、両者間で一致する値が存在する旨の判定が下されたとき、特定の番組に係る視聴権が存在するとみなして、蓄積されたスクランブル信号に対してデスクランブル処理を施すことで特定の番組に係る原信号を復元することにより、特定の番組の蓄積型視聴を許可するので、したがって、第2の特定回数から第1の特定回数を減算することで得られた回数制限下で蓄積型視聴が許可される結果として、蓄積型視聴を行う場合であっても、放送事業者側の意図に反した番組視聴を可及的に抑制可能な放送受信システムを得ることができるというきわめて優れた効果を奏する。

【図面の簡単な説明】

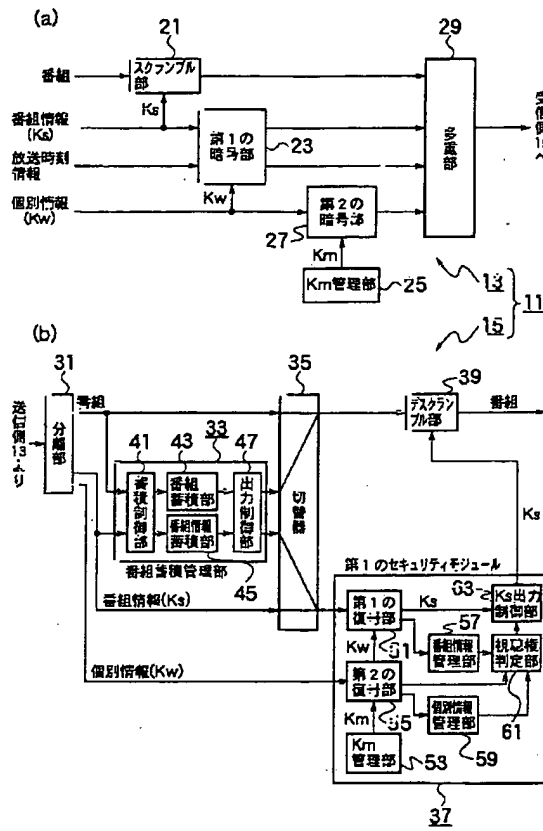
【図1】図1は、本発明に係る第1乃至第2の放送受信方法が適用される、第1乃至第2の放送送信装置、及び第1乃至第2の放送受信装置を含んで構成される第1乃至第2の放送受信システムの機能ブロック構成図である。

【図2】図2は、本発明に係る第3の放送受信方法が適用される、第3の放送送信装置、及び第3の放送受信装置を含んで構成される第3の放送受信システムの機能ブロック構成図である。

【符号の説明】

- 11 第1乃至第2の放送受信システム
- 13 第1乃至第2の放送送信装置
- 15 第1乃至第2の放送受信装置
- 21 スクランブル部
- 23 第1の暗号部
- 25 Km管理部
- 27 第2の暗号部
- 29 多重部
- 31 分離部
- 33 番組蓄積管理部
- 35 切替器
- 37 第1のセキュリティモジュール
- 39 デスクランブル部
- 41 蓄積制御部
- 43 番組蓄積部
- 45 番組情報蓄積部
- 47 出力制御部
- 51 第1の復号部
- 53 Km管理部
- 55 第2の復号部
- 57 番組情報管理部
- 59 個別情報管理部
- 61 視聴権判定部
- 63 Ks出力制御部
- 101 第3の放送受信システム
- 103 第3の放送送信装置
- 105 第3の放送受信装置
- 111 数値生成部
- 113 第2のセキュリティモジュール
- 115 数値生成部
- 117 数値プール部

【図1】



【図2】

